Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB05/001709

International filing date: 04 May 2005 (04.05.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/659,133
Filing date: 07 March 2005 (07.03.2005)

Date of receipt at the International Bureau: 31 May 2005 (31.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

GB05/1709

PA 1302118

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 01, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/659,133***
FILING DATE: ***March 07, 2005***

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

L. Edelen

L. EDELEN
Certifying Officer

Please type a plus sign (+) inside this box → [+]

PTO/SB/16 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
John Flemming	WALKER	United Kingdom

☐ *Additional inventors are being named on th____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (280 characters max)

CHIP SHIELDING SYSTEMA ND METHOD

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer Number 24628 →

OR

Type Customer Number here

Place Customer Number Bar Code Label here

☒ Firm *or* Individual Name	L. Friedman				
Address	Welsh & Katz, Ltd.				
Address	120 S. Riverside Plaza, 22nd Floor				
City	Chicago	State	Illinois	ZIP	60606
Country	USA	Telephone	312-655-1500	Fax	312-655-1501

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 11

☒ Drawing(s) *Number of Sheets* 2

☒ Application Data Sheet. See 37 CFR 1.76

☐ CD(s), Number

☒ Other (specify) Fee transmittal; certificate of Express Mailing EV555564359US

Total # of sheets 13 = Application Size Fee $0.00

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

☒ A check or money order is enclosed to cover the filing fees

☒ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 23-0920

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) $200.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME L. Friedman

TELEPHONE 312-655-1500

Date 7 March 2005

REGISTRATION NO. 37,135 *(if appropriate)*

Docket Number: 7251/93878

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

P19LARGE/REV07

Doc Code:

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL for FY 2005

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) $200.00

Complete if Known	
Application Number	
Filing Date	7 March 2005
First Named Inventor	Walker
Examiner Name	
Art Unit	
Attorney Docket No.	7251/93878

METHOD OF PAYMENT (check all that apply)

☒ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☐ Deposit Deposit Account Number: 23-0920 Deposit Account Name: Welsh & Katz, Ltd.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or any underpayment of fee(s) under 37 CFR 1.16 and 1.17 ☒ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	$200.00

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 20 or HP =	_____ x	$50.00 =	$0.00

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
_____ - 3 or HP =	_____ x	$200.00 =	$0.00

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)
_____	_____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listing under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
_____ - 100 =	_____ / 50	_____ (round up to a whole	x $250.00 =	$0.00

4. OTHER FEE(S)

	Fee Paid ($)
Non-English specification, $130 fee (no small entity discount)	_____
Other (e.g. late filing surcharge): _____	_____

SUBMITTED BY

Signature		Registration No. (Attorney/Agent)	37,135	Telephone	312-655-1500
Name (Print/Type)	L. Friedman			Date	7 March 2005

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Patentee: WALKER
Title: CHIP SHIELDING SYSTEM AND METHOD
Serial No.:
Filing Date: 7 March 2005
Docket No. 7251/93878

Certificate of Express Mailing

Express Mail mailing label number EV 555564359 US

Date of Deposit: 7 March 2005

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail" Post Office to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. This mailing includes Provisional Application Cover Sheet (1 pg); Fee Transmittal (1 pg) in duplicate; Check in the amount of $200.00; Specification (11 pgs); Drawings (2 sheets); Application Data Sheet (2 pgs); and return receipt postcard.

The person mailing this paper is:

Shannon Wooten
Typed or Printed Name of Person Mailing Paper of Fee

Signature of Person Mailing Paper or Fee

CHIP SHIELDING SYSTEM AND METHOD

FIELD OF THE INVENTION

The present invention relates to protecting integrated circuit chips from invasive attack through the use of a shield.

BACKGROUND OF THE INVENTION

Security chips are of use to those wanting to protect information, data transmissions or value (typically monetary). These security chips protect data by storing it in secure memory or transmit data securely through the use of cryptography implemented on chip. There are many reasons for using these products including secure banking cards, secure access systems and secure personal identity systems. It is known in the art to protect these chips from invasive attacks whereby criminals and other agents attack the card to try to obtain, change or use secret information on the card.

One type of attack involves trying to place contacts onto internal chip nodes in order to read internal data traffic. This may be achieved by probing, using fine needles to break through the surface passivation to reach the fine metal tracks. Alternatively focused ion beam (FIB) may be used to deposit pads of metal onto the tracks for subsequent probing or bonding by wires. However it is achieved, measuring the signals on internal chip nodes represents an attack, and if successful this attack may render the chip and entire system on which it is based, insecure.

Shields to protect a chip from the above attacks exist at present; they are typically divided into two categories, active and passive. Passive shields are simple metal layers over all or part of the circuit and are designed to prevent viewing and probing. Passive shields may be removed by chemical, plasma or other techniques without changing the operation of the circuit. In other words, a passive shield works to deter attackers by making viewing more difficult initially, but will not actively defend itself against removal.

Active shields may look similar or may look more like a network of lines covering all or part of a circuit. If a line or part of the shield is removed,

severed or short-circuited to another line, the breach is detected and the chip halts some or all functions.

Active shields may still be breached using, for example, the following technique. An active shield line is identified as above the circuit element to be attacked. The shield line is bypassed using the ability of the FIB system previously mentioned. The bypass is in the form of a diversion track added in parallel to the original shield track. The original shield track may now be removed leaving the new bypass to fool the detection circuit. No circuit break is detected.

The following references are believed to represent the state of the art:

US Patent No. 4,583,011 to Pechar;

US Patent No. 4,766,516 to Ozdemir et al;

US Patent No. 4,920,402 to Nakaya et al;

US Patent No. 5,336,624 to Walden;

US Patent No. 5,468,990 to Daum;

US Patent No. 5,783,846 to Baukus et al;

US Patent No. 5,866,933 to Baukus et al;

US Patent No. 5,821,582 to Daum;

US Patent No. 5,824,571 to Rollender et al;

US Patent No. 5,930,663 to Baukus et al;

US Patent No. 5,973,375 to Baukus et al;

US Patent No. 6,064,110 to Baukus et al;

US Patent No. 6,117,762 to Baukus et al;

US Patent No. 6,294,816 to Baukus et al;

US Patent No. 6,360,321 to Gressel et al;

US Patent No. 6,613,661 to Baukus et al;

US Patent No. 6,720,656 to Matsumoto;

US Patent Application Publication No. 07/923,411 of Baukus et al;

US Patent Application Publication No. 2001/0033012 of Koemmerling et al;

US Patent Application Publication No. 2002/0173131 of Clark JR et al;

PCT Published Patent Application WO 97/29567 of Fortress U & T Ltd.;

PCT Published Patent Application WO 01/50530 of Koemmerling et al;

PCT Published Patent Application WO 01/54194 of NDS Limited;

EP Published Patent Application No. EP 0 585 601 of Hughes Electronics Corporation;

EP Published Patent Application No. EP 0 940 851 of Hughes Electronics Corporation; and

"*Infineon Introduces Chip Card Controllers for Improved Security of Electronic Identity Cards and Passports*", available on the World Wide Web at www.infineon.com/cgi/ecrm.dll/jsp/showfrontend.do?lang=EN&BV_SessionID=@@@@0590998578.1109855404@@@@&BV_EngineID=ccchadddmlfiddkcflgcegndfifdfoh.0&content_type=NEWS&content_oid=107623&news_nav_oid=-9979.

The disclosures of all references mentioned above and throughout the present specification, as well as the disclosures of all references mentioned in those references, are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention, in preferred embodiments thereof, comprises an active shield made in such a way that individual tracks are not visible by any normal microscopy technique. The tracks are preferably present in a layer of semiconductor material. The tracks preferably comprise doped regions separated by semi-insulating regions of either undoped material, or differently doped material. The tracks are doped sufficiently to allow conduction of electronic carriers. Between the tracks, the material, doped or undoped, is depleted of carriers. This region is rendered semi-insulating through the lack of intrinsic or extrinsic carriers, or through the trapping of such carriers. The conductive region is formed into tracks which form part of an active shield as described above. Most preferably, the conductive lines and the insulating regions between them are made in the same way and look identical to all analytical techniques. An attacker therefore does not know where to bypass the active shield lines.

Preferably the path of the conductive tracks is randomized for each shielded chip produced. The randomization helps prevent attackers from characterizing a device destructively to find the shield path, and then applying the information gained to a pristine device. Shield breach detection circuitry is preferably added to the circuitry of the chip, so that when a breach in the active shield is detected, the detection initiates a "breach detected" mode designed to protect the chip from reverse-engineering, as is well-known in the art.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 2 is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention, in preferred embodiments thereof, provides a method to protect a security chip from invasive attacks. Preferably, a layer is added above the layers of the circuit to be protected from attack. The added layer may be made of polycrystalline silicon, as this material is commonly used in the manufacturing cycle of integrated circuits, but may alternatively be made of many other suitable materials. Any material whose conductivity can be materially changed without being visibly different would be a candidate for the material to be used in the added layer. The added layer is typically applied towards the end of the chip manufacturing process, and is applied above the normal circuit interconnect layers. The added layer may also be protected by a passivation layer, as is typically used in such integrated circuits.

The added layer is preferably implanted with dopants to allow conduction.

In a first preferred embodiment of the present invention, dopants are selectively implanted in tracks corresponding to where the designer wants them placed, as follows:

- A layer of photo-resist is placed on top of the newly added layer, and the desired pattern of tracks is created in the photo-resist by any appropriate method, such methods being well-known in the art.

- The photo-resist is developed, leaving the desired track pattern bare, with the rest of the wafer being still covered by photo-resist.

- Dopants may then be implanted in the material by high energy ion bombardment or by any other appropriate method. Dopants are thus implanted in the desired pattern of tracks (and also, incidentally, in the photo-resist).

- The photo-resist is then removed from the wafer, leaving the dopants selectively implanted in the desired pattern of tracks.

In a second preferred embodiment the present invention utilizes either blanket bombardment of the layer with dopant ions or incorporation of the dopants during the growth of the layer. The latter approach will typically be achieved in the case of doped polysilicon, by chemical vapor deposition (CVD)

growth using silane gas for silicon growth and boron trichloride gas for dopant species.

However the growth and dopant incorporation is achieved, it must be done in such a way that the incorporated dopant atoms are not active. This means that the dopant atoms are not on designated sites as substitutes for the main material atoms. This means that the dopant atoms are interstitial, or between their normal, substitutional sites. This further means that the dopant atoms do not contribute carriers to conduction processes in the layer. This means that the material, as grown, is semi-insulating and does not conduct.

A further step in the creation of the shield layer is the activation of the dopants described above. The activation is typically achieved through an annealing process. This annealing process is effective if the material is heated to a temperature close to (typically, within approximately 100 degrees C of) its melting point.

In the first preferred embodiment described above, annealing of the entire wafer (blanket annealing) will cause the implanted tracks to become conductive; such blanket annealing may be carried out using any appropriate method known in the art.

In certain preferred embodiments of the present invention, the doped polysilicon is rapidly brought up to the annealing temperature by irradiation from a pulsed light source. The pulsed light source may be an infrared laser. The laser may be a YAG laser (Yttrium Aluminum Garnet, output wavelength 1064 nm). This laser may be driven in pulsed mode with a q-switch to limit the on-time to several nanoseconds or faster. The high power density during the pulse must be sufficient to anneal the dopants in that region of the material. In addition, the power density during the pulse must not be sufficient to ablate the material or cause damage to active circuit layers. Such laser annealing is preferred in the second preferred embodiment described above.

In the second preferred embodiment described above, conductive tracks are preferably patterned into the layer by the laser annealing action. The laser, for example, may be scanned across the surface. The pattern of scanning is immaterial but may be raster scanning or following the semi-random path of a

tracks path from start to end, or most efficiently, by alternate direction scanning (boustrephorous scanning) of the surface. The annealing will locally activate the dopants in the tracks required.

The annealing must be such that the conductive tracks are physically similar in all important respects to the semi-insulating material between the tracks. An attacker cannot "see", by normal analytical means, the tracks to be bypassed in an attack.

In certain preferred embodiments of the present invention, in order to further frustrate attackers, the path of the conductive tracks is randomized for each shielded chip produced. The randomization helps stop attackers from trying to characterize a device destructively to find the shield path, then applying the information gained to a pristine device. The additional effort required to randomize the path is preferably implemented in control software and is thus independent of processing hardware.

Randomization in this case may mean annealing to form the conductive tracks using straight lines and 90-degree bends (although it is appreciated that it is not necessary to use straight lines and 90-degree bends), but would be random in how the conductive path connects one contact to another. For example, in one chip, one may use the simplest path between two points - a straight line. In another chip the same two contacts could be joined by a longer series of meanders, and in other chips by different series of meanders. The point, as stated above, is to prevent a hacker from discovering the path of the shield in one device and using the path information to bypass the shield in all other devices of the same series of chip.

Even though each chip would have the shield conductive paths in different patterns, the end contacts would preferably be in the same place in each chip, since photolithographic masks, which are difficult to change, define the locations of the contacts. Manufacturing many different copies of photolithographic masks would be extremely expensive. Therefore, the preferred track "writing" process is serial, enabling each chip to be different without incurring the difficulties inherent in changing the photolithographic masks.

Typically, the conductive paths are connected to underlying circuitry using conventional techniques such as tungsten plug vias, one at each end of each conductive path. It is also expected that, for additional security, dummy vias, as are known in the art, will be present but unused. The addition of dummy vias is intended to foil attempts to penetrate the shield layer based on guesses as to which vias may be bridged to bypass a conductive path. The creation of diversion tracks based on erroneous guesses preferably initiates circuit modes that prevent the chip from operating correctly, as is well-known in the art.

It is appreciated that the control software driving the track annealing process could be programmed to route the conductive tracks automatically by driving the laser with randomly added deviations from a simple path from one track end to the other track end. An alternative and perhaps simpler technique is to have a large but fixed number of conductive path patterns, and to make a random choice of which pattern to use for each chip.

Reference is now made to Fig. 1, which is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention. This figure shows the basic construction of an integrated circuit with a silicon (single crystal) substrate on top of which are constructed gates and other active and passive circuit elements interconnected by networks of (typically) aluminum tracks. As these aluminum tracks are vulnerable to attack a layer of polysilicon is shown above them to illustrate the position of the protective shield layer.

Reference is now made to Fig. 2, which is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1. This figure shows a top down view of the protective shield layer. The serpentine track illustrates one method, as described above, of writing a serpentine conductive line in this material. As described above, this can be achieved by scanning a pulsed infra-red laser over the areas to be annealed. The annealing activates the dopants in this region, allowing conduction along the track. The track may be connected to the underlying circuitry using, for example, tungsten plugs as vias.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in

combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

What is claimed is:

CLAIMS

1. Apparatus substantially as described hereinabove.

2. Apparatus substantially as shown in the drawings.

3. A method substantially as described hereinabove.

4. A method substantially as shown in the drawings.

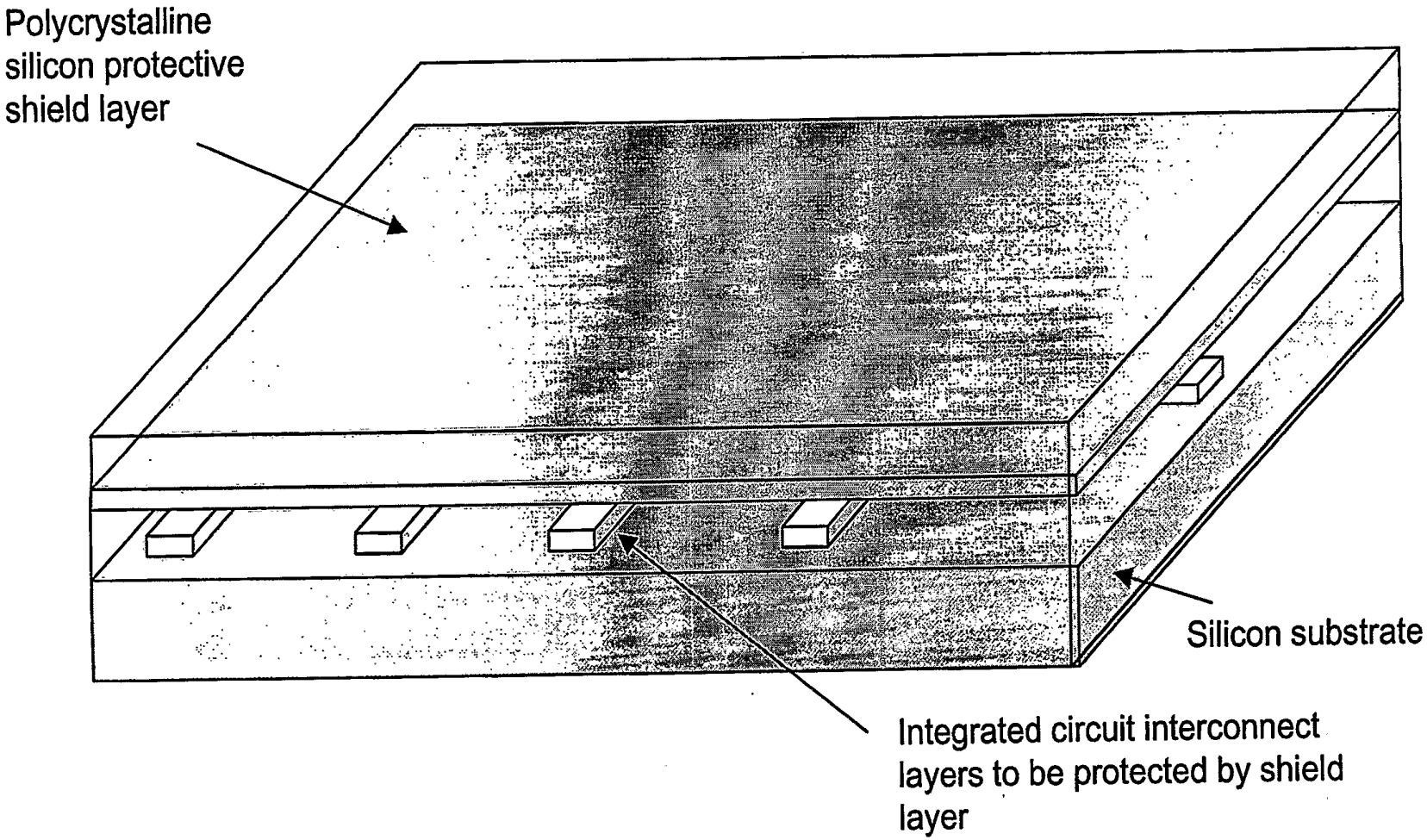

Fig. 1

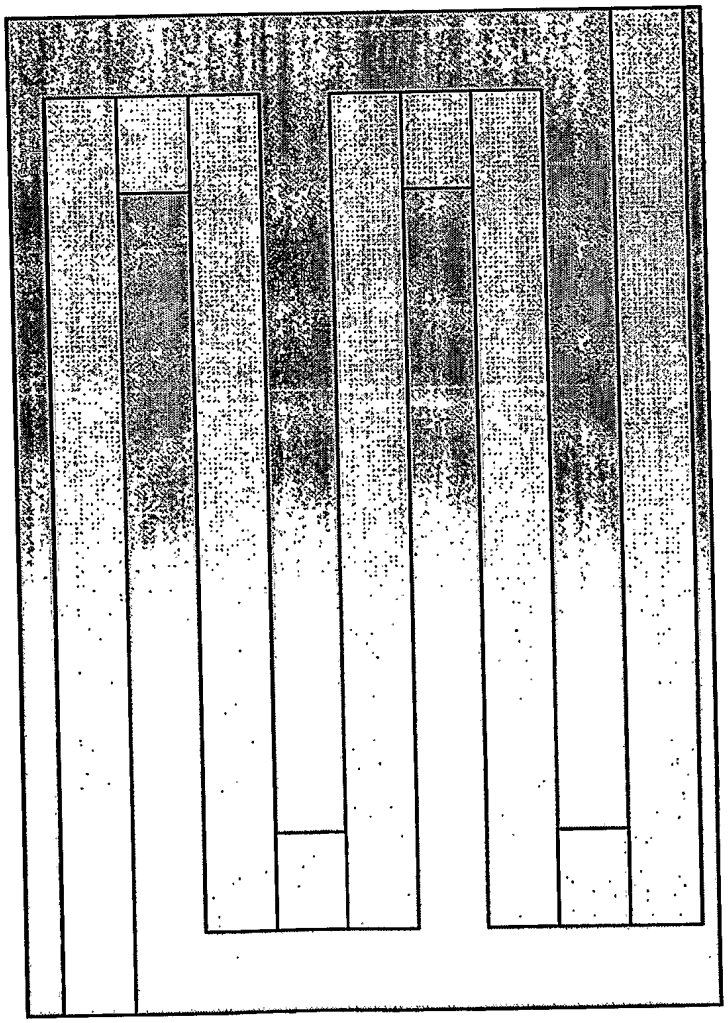

Fig. 2

Application Data Sheet

Inventor Information

Inventor One Given Name::	John Fleming
Family Name::	WALKER
Postal Address Line One::	1 Malyns Close
City::	Chinnor, Oxon
Country::	United Kingdom
Postal or Zip Code::	OX39 4EW
Citizenship Country::	United Kingdom

Correspondence Information

Name Line One::	Welsh & Katz, Ltd.
Name Line Two::	L. Friedman
Address Line One::	22nd Floor
Address Line Two::	120 South Riverside Plaza
City::	Chicago
State or Province::	Illinois
Postal or Zip Code::	60606
Telephone Number::	(312) 655-1500
Fax::	(312) 655-1501

Application Information

Title Line::	CHIP SHIELDING SYSTEM AND METHOD
Total Drawing Sheets::	2
Application Type::	Provisional
Docket Number::	7251/93878

Representative Information

Representative Customer Number: 24628

Assignee Information

Assignee Name: NDS Limited

Assignee Address: One London Road
Staines, Middlesex TW18 4EX
United Kingdom